

GENI Clearinghouse Policy

Name: GENI Clearinghouse Policy
Author: Adam Slagell
Version: 0.4.2 (Working Draft)
Date: Jan 12, 2012

1. Goals & Scope

This is a policy document (1) describing to the GENI federation actors (a group of people and institutions pooling resources to perform wide area network experimentation) what the GENI clearinghouse is, (2) the services it will provide, and (3) the policies it will follow to operationally meet the needs of the community. The GENI Oversight Group, a committee formed from multiple federation stakeholders (e.g., aggregate authorities, identity portals, GENI operations, project leaders, campus representatives, and the GPO), directs the mission and operation of the clearinghouse.

The different actors in GENI have both social needs, which the clearinghouse serves a legal entity, and technical needs, which the clearinghouse meets as a provider of services. For example, project leaders (those responsible for the creation of official GENI slices affiliated with a particular set of experiments, analogous to principal investigators) want to know what it means to be a project leader and what kind of service they can expect by running experiments on GENI aggregates. Aggregate authorities want to know that someone trustworthy and identifiable is in control of experiments running on their resources. Rather than signing many pairwise agreements between thousands of entities, these parties join the GENI federation by both entering into common agreements with the GENI clearinghouse. These agreements clarify for different actors what actions they are taking responsibility for and the principles by which they are operating their services. Therefore, joining the federation provides a simple way for everyone to reach a common understanding of their roles, while only agreeing to a minimal set of principles needed for smooth and friendly operations.

There is also a technical-side to all of this. Someone has to vouch for these different actors so that everyone knows whether or not they are collaborating with someone who has agreed to this common set of policies and agreements. This is done through the concept of GENI-registered slices and projects, which are precisely those endorsed by the clearinghouse. An endorsement (or attribute statement) from the clearinghouse is thus a marker that all parties have agreed to this common set of policies. Therefore, the primary services of a clearinghouse are (1) to register projects and bind them to project leaders, (2) to provide mechanisms to allow the proper binding of these projects to slices involving only parties (identity portals, slice authorities, project leaders and experimenters) who have signed agreements with the clearinghouse (i.e., slice registration), and (3) to identify for experimenters and slice owners officially endorsed GENI aggregates (i.e., those who have signed the GENI Aggregate Provider Agreement).

The clearinghouse also provides many secondary services which are not critical to its primary role of establishing a common set of policies for GENI actors and a way to recognize each other. Those who choose to enter into common agreements with the clearinghouse may also benefit from:

- an identity portal providing GENI principal registration and credential issuance;
- a slice authority providing the ability to mint (separate from registering) GENI slices;
- federation resource allocation policy verification (aka slice tracker); and
- a set of web portal services to make experiment management simpler.

This policy document and the referenced agreements do not preclude any bilateral agreements between experimenters, aggregate authorities, identity providers and other GENI service providers, though. No one is required to sign any agreements to use GENI software and architectures, but they may (1) lose the services of the clearinghouse and GENI Operations and (2) will not have their slices or aggregates endorsed as official GENI resources through the attestation of the clearinghouse.

2. Related Documents

These related documents contributed strongly to our understanding of what the GENI Clearinghouse is: its roles, responsibilities and services provided. A changing and developing understanding of GENI's architecture or the federation's organization may result in changes to this concept of clearinghouse operations. Any such changes will require the definitions in this document to be updated, and their impact on the principles espoused here will have to be determined.

Document ID	Document Title and Issue Date
GeniSysOvrw	"GENI System Overview", September 29, 2008. http://groups.geni.net/geni/wiki/GeniSysOvrw
SysReqDoc	"GENI System Requirements Document", July 7, 2009. http://groups.geni.net/geni/wiki/SysReqDoc

ExperimentLifecycleDocument	"Lifecycle of a GENI Experiment", April 30, 2009 http://groups.geni.net/geni/wiki/ExperimentLifecycleDocument
GEC 11 Slides	"Federation in GENI & the GENI Clearinghouse", July 27, 2011 http://groups.geni.net/geni/attachment/wiki/GEC11Federation/GENI%20Federation%20-%2022July2011.pdf
Aggregate Provider Agreement	"Aggregate Provider Agreement", Oct. 10, 2010 http://groups.geni.net/geni/attachment/wiki/ComprehensiveSecurityPgm/Aggregate%20Provider%20Agreement?

3. GENI Federation Actors & Agreements

For all the actors below, the clearinghouse maintains the authoritative registry simply because **the members are defined by those who have entered into common agreements with the clearinghouse**. It is desirable that one be able to prove membership, i.e. that one has signed an agreement with the clearinghouse, asynchronously and offline. The table below describes the purposes of these registries and whether or not they are public or private. Below that we describe the roles for these different actors that make up these registries more thoroughly.

Registry	Public/Private	Use
Aggregate Provider	Public	Slice owners can determine who has signed the Aggregate Provider Agreement with the clearinghouse. This need not be publicly queryable if another mechanism, such as ABAC, allows slice owners to determine such endorsement. However, it may still be useful to provide for discovery purposes if one wants to find only endorsed aggregates and components quickly.
Identity Portals	Public	Experimenters can discover places to create GENI identity credentials that will be recognized by the clearinghouse. Again, it doesn't need to be publicly queryable to determine if an IdP is endorsed, but it is useful to have such an open registry for first time users wanting to know where it get credentials.
Slice Authorities	Public	Experimenters can discover places to create GENI slice credentials that will be recognized by the clearinghouse. This does not need to be queryable for one to determine whether or not a slice authority is endorsed, but it is useful for users to have a list to go to if they want to create their first slice.
Experimenters	Private	Aggregates can be assured slices endorsed by the clearinghouse are run by those who have accepted the GENI AUP for experimenters. The list may not be complete at the clearinghouse as it can delegate responsibilities to trusted identity portals and slice authorities.
Project Leaders	Private	Aggregates can be assured slices endorsed by the clearinghouse are associated with projects run by a responsible project leader who takes ownership for their slices and has entered an agreement with the clearinghouse. This registry binds projects to registered project leaders.

Aggregate Providers

The aggregate providers are vital to the community as they are providing all the resources (e.g., virtual machines, routers, network links, etc) for experiments in GENI. Because of their importance, and because the aggregates appeared before even the users, an **Aggregate Provider Agreement** was developed early on. This agreement sets a baseline of expectations for the behavior and responsibilities of GENI aggregates. Experimenters building slices will know that resources attested to by the clearinghouse are those of the aggregates which have signed off on this agreement. Aggregates seeing requests for resources from slices endorsed by the clearinghouse will know that they are dealing with users who have signed off on a GENI Acceptable Use Policy.

While an initial Aggregate Provider Agreement was approved at earlier GECs, it has been updated to reflect new language and concepts that have developed along with this conception of the clearinghouse. As refinements to the clearinghouse concept continue, all agreements may need more updates.

This endorsement of aggregates could be implemented as a trusted directory services that also supports resource discovery for experimenters, or this registry could be private, in which case aggregates would need to be signed in a way that slice owners could verify that aggregates are "GENI-approved", perhaps with ABAC credentials. These solutions need not be mutually exclusive, though.

Identity Portals

The concept of multiple identity portals (each using approved identity providers) for GENI is relatively new, at least in its formal conception. Campuses, through InCommon, and other testbeds (e.g. Emulab/ProtoGENI) will all act as identity portals, collecting/passing attributes, issuing credentials and revoking credentials. The clearinghouse is also an identity portal, which will rely on InCommon for authentication and possibly some additional attribute collection. Agreements between the clearinghouse and different identity portals may have to be customized based upon the services provided. However, each agreement will have to address common issues such as using an appropriate backend identity provider, having revocation capabilities for long term credentials, retaining logs, and collecting/passing the proper types of attributes.

A slice authority could be considered a special type of identity provider which requires a different sort of agreement. If a slice is not created by the clearinghouse, there must still be a way to map slices to real people. The clearinghouse, when registering and signing such a slice, is trusting that the slice authority is (1) logging all transactions of slice creation, (2) maintaining a mapping of slice creators to principals (note, this is implicit in current ProtoGENI slice credentials), (3) creating slices only for users from a valid GENI identity portal who has presented to users a GENI AUP (as long as the slice credential contains the slice owner's credential this can also be verified by the clearinghouse), and (4) maintaining

an ability to revoke slices **if slice credentials are valid for more than 24 hours**. All four of those points are important parts of an effective agreement with a slice registry and must be present, even if they are wrapped up as part of a larger identity portal agreement instead of a separate slice authority agreement.

As we will note later, this whole slice registration service of the clearinghouse could also be delegated to slice authorities using ABAC towards the same ends. In that case, these agreements will have to specify that the slice authorities respect the appropriate ABAC policy.

Experimenters

While there is a Recommended Use Policy for users in GENI, there is *currently* no formal Acceptable Use Policy (AUP). Further, the RUP is not actually presented to anyone. For many reasons, it is important that a formal AUP be presented to users upon registration and before they are issued any GENI credentials. Users want to know what is expected of them, what behaviors they may be held responsible for, what rights they have, and how they could redress actions taken against them by others in the federation. Similarly, resource providers want to know that experimenters are taking responsibility for their actions and are acting in concordance with common sense expectations as one who is providing free resources to the experimenters. Agreeing to these principles gains the experimenter access to a wider set of resources for their experiments with minimal burden.







The AUP should start with the RUP and be created by a group derived from both the user and resource provider communities. It should cover minimal but important expectations, such as, "users will follow all applicable laws and regulations". It should also clarify to experimenters that they are responsible for the behavior of their experiments. Furthermore, an understanding of proper treatment towards opt-in users and the need to register any software they install on opt-in user systems should be explicated here. For example, experimenters should respect the privacy of opt-in users and their wishes to no longer be a part of an experiment. Lastly, this AUP should reference the Legal, Law Enforcement and Regulatory (LLR) Plan, which was derived after the RUP was written.




Project Leaders

Project Leaders may be users themselves, but need not be the ones creating slices and actually running experiments. For example, a PI may simply delegate the ability to create slices for the project to a graduate student without actually configuring the experiment herself. However, they still have responsibilities as the ones who guide projects and delegate the ability to bind slices to projects. Therefore, they need to register with the clearinghouse, and any slice that is to be attested to by the clearinghouse must be tied back to a registered project and project leader. The way this will work is that the clearinghouse will give the project leader a project credential (or attribute). The project leader can use that credential to delegate the ability to create slices for that project to another user. That user will create a slice with a valid slice authority. To register the slice with the clearinghouse, the slice creator will need to present the delegation credential along with the slice credential to the clearinghouse, perhaps with some additional self-certified information requested at that time (This could be delegated to slice authorities if as part of their agreements they run the same checks prior to issuing a slice credential and agree to share key information with the clearinghouse if requested). Only the clearinghouse can bind a project to a project leader, though how this is implemented is outside of this policy.

The project leader has ultimate responsibility for all the slices associated with their project. Therefore, an agreement should be presented to the project leader, when registering with the clearinghouse, which has all the content of the AUP, but additionally holds them responsible for being truthful in the project description. It must also make them aware of their responsibility for all the project's slices, and hence the importance of not carelessly delegating the authority to register slices with the project. This is important because it is not technically possible to determine all of the experimenters who may have the ability to work within a slice, but only possible to determine the slice creator and project leader.

Status of Discussed Federation Agreements and Plans

-  Aggregate Provider Agreement
-  Identity Portal Agreement
 - *No IdP agreements have been created, but GENI will need ones with ProtoGENI & Planetlab at a minimum. Agreements may also be needed in the future with FIRE, DETER and ORCA. Each will be unique, but I could imagine two or three basic templates.*
 - *Should have things like having the GOG suspending a user means that they do not create GENI credentials for that user and revoke current ones.*
 - *Present AUP to new users*
-  Slice Authority Agreements
 - *These might be rolled into IdP agreements since it seems one is unlikely to be an authorized slice authority if not an IdP.*
 - *SAs need to log transactions: slice credential, associated identity credentials, project ID and any relevant delegation credentials, timestamps, IP addresses, and the results of all the verification steps."*
 - *SAs need to keep track of resources granted to their slices, especially since notices to the CH from aggregates is likely best effort.*
 - *CA policies like short-lived certificates, maintaining CRL are important. Lifetime is more important than the CRL since revocation is only going to be checked when resources are granted and can't shutdown a slice.*
 - *ABAC policies may need to be made specific if the CH delegates slice registration to trusted SAs.*
-  Project Leader Agreement
 - *There is none, but this is not needed until there is a functional clearinghouse. Similar to an AUP, but really places emphasis on their responsibility as owner of slices and experiments.*
-  Federation Charter
 - *There should be a federation charter that describes the governance structure of GENI and references all the agreements in this subsection. This section will then be less relevant in this document, and some of the policies (e.g., how disputes are resolved between actors) should be moved there.*
-  Acceptable Use Policy

- *There is none, but one could and should be created soon based off of the RUP. Perhaps more thought is needed on opt-in user issues, though.*
 - way to opt out
 - inform if they are going to install software on user system (both LLR & User)
 - respect privacy, be clear about how data will be used
- *Need to say what can happen for violating an agreement. What is the process to get to such a consequence, and how can it be appealed?*
- *be responsible for software on their slice, debug before deploying large scale experiments.*
 - *not responsible is running very insecure software that could allow an experiment to be hijacked*
- *net etiquette, avoid disruption of shared resources*
 - *cooperate in resolving disruptions*
- *no illegal activities*
- *cite geni in pubs*
-  Legal, Law Enforcement & Regulatory Plan
-  [Clearinghouse Policy](#)
-  Incident Response Plan
 - *It is in an early draft form, but it cannot be implemented without some decisions being made, positions created and funding allocated. The last section should inform future projects to be funded, though.*

4. Clearinghouse Services

Project Creation

Every experiment and every slice in GENI will be associated with a GENI Project. For a slice to be registered with the clearinghouse, it must be bound with an official project.

The clearinghouse will provide an interface that allows projects to be registered and approved. While the clearinghouse will delegate to identity providers the ability to define who has the project leader attribute, project leaders must still register an account with the clearinghouse before they can create new projects. They can either have the clearinghouse mint a GENI identity credential for them with the assistance of one of its identity providers (e.g. InCommon), or they could authenticate with a GENI identity credential issued by an approved GENI identity portal (e.g., ProtoGENI) assuming they can prove their project leader attribute. Additional attributes (see attribute subsection) may be collected and verified by clearinghouse operations staff at this time (e.g., contact information).

Once a clearinghouse account has been created for the project leader, bound to a valid GENI identity and verified, a project leader can create one or more projects. Projects will have a unique ID as well as a common name. When making the request they will briefly describe the project purpose, whether or not it will utilize opt-in users, where they would like project emails forwarded, and any special needs the project may have (e.g., exclusive use of critical GENI infrastructure or a large part of it for a conference). Project leaders will be able to come back and update any information entered here, and furthermore it would be useful to send out reminders for project leaders to update this information from time to time. While for convenience the clearinghouse developers may wish to give an option to add delegations for slice creation at this point, that would be optional and not really part of the project creation process.

After the successful registration of a project, the project leader will receive a signed project credential or attribute allowing them, or their delegates, to register slices (i.e., bind slices to projects) associated with the project. Of course, to register such slices, they must be created by a principal registered at the clearinghouse or another authorized GENI identity portal. Further, the slice must be created at either the clearinghouse or another endorsed GENI slice authority. This ensures that the creator of the slice is tied to a GENI principal at the clearinghouse or one of the other trusted identity portals. Without this, a slice seeking endorsement from the clearinghouse (i.e. registration) could be owned by someone who has never seen an AUP and with a slice authority that keeps no proper records of slice creation.

Principal Registration & Revocation

Experimenters can create a GENI account and obtain GENI identity credentials through the clearinghouse. Using an identity provider, such as InCommon, they can authenticate to the clearinghouse. If additional attributes not provided by the identity provider are needed, they will be supplied by the experimenter and verified manually by the clearinghouse operators. Because of the need to manually verify attributes, at least during early operations, the clearinghouse will work to get accounts approved and credentials issued within two business days.

Other endorsed GENI identity portals, having entered agreements with the clearinghouse, will be able to mint the GENI identity credentials themselves, but they must support revocation and present new users with the GENI AUP (Acceptable Use Policy) before issuing credentials. Furthermore, an identity portal that creates GENI credentials for principals must log that transaction so that it can be determined when the AUP was presented to the user. When acting as an identity portal, the clearinghouse will also log each new account creation, presenting the AUP to users before allowing the application process to complete. It will record a pointer to the principal record, timestamp of issuance, and the remote IP address from which the account request came.

For all credentials issued at the clearinghouse, there must be a mechanism for revocation of compromised credentials. Furthermore, users may have their accounts revoked for violating the AUP (the process by which that could happen or be appealed is to be in the AUP). In either case, there must be a prompt mechanism for revocation, **or use of very short-lived certificates**. For credentials lasting more than 24 hours, the clearinghouse will maintain a Certificate Revocation List (CRL) that is referenced in any credential issued. Ideally, the clearinghouse would also support OCSP for real-time revocation information, though that would not be required of all identity portals. Only support of a standard revocation mechanism is required in the agreements with them.

Slice Creation and Registration and Revocation

Any approved GENI slice authority (whether the clearinghouse's own slice authority service or another which has entered into agreements with the clearinghouse) can mint slice credentials for GENI if they agree to log the transactions, record the slice owner, and support revocation of the slice credentials lasting longer than 24 hours. However, to be registered with the clearinghouse and associated with a project, the following steps must be followed:

1. **Slice authority verified:** It is verified that the slice credential is in good status and from a source trusted to mint slices, one that follows certain best practices and maintains appropriate logs (Of course, this is only applicable if registration is happening at the clearinghouse and not the slice authority that mints the slice which would already need to be endorsed by the clearinghouse to successfully register a slice).
2. **GENI identity credential verified:** It must be verified that the slice owner's credential is in good status and was issued by an endorsed identity portal (i.e., one that has signed an agreement to collect and verify attributes, uses approved identity providers, presents users with the AUP, and logs credential creation).
3. **Project verified:** The slice registration request must ask for registration to bind the slice to a valid project. Furthermore, the slice creator must either be the project leader or someone who can prove that they have been delegated the right to mint slices for that project.
4. **Slice information collected:** The creator describes the purpose of the slice and experiments on it and fills in contact information to which the slice specific email alias will be mapped.
5. **Slice credential is signed:** The verifier signs the slice credentials in a way that binds it to the project or creates the proper attribute credential.

This whole process is logged, including any credential/attribute generation. The slice credential, associated identity credentials, project ID and any relevant delegation credentials are logged. Timestamps and IP addresses are also recorded, as well as the results of all the verification steps. These logs are retained and protected as specified in the privacy and logging policies of the clearinghouse. Other verifiers, should it be delegated to slice authorities, will need to make clear their privacy policies. If the slice credential was issued by the clearinghouse, it will maintain a list of all resources allocated to the slice in its slice registry (this information is pushed to the clearinghouse's slice authority service from the aggregates). In other cases, the clearinghouse may rely upon another slice authority to maintain this information, who as part of their agreement with the clearinghouse agrees to also log such information.

A CRL will be maintained that allows revocation, i.e. deregistration, of slices lasting more than 24 hours. If the clearinghouse issued the slice, it can also revoke the slice credential itself, too. An automated proxy renewal service could be used to renew slice credentials and even re-register them with the registrar.

It should be noted that if slice authorities agree to do these same checks, then all of this could be done with ABAC and delegated to the slice authorities. The clearinghouse need not be a bottleneck. Of course, the agreements would require the SAs to not only perform these checks before creating/registering a slice and giving it an official GENI endorsement, but they would also need to agree to log all of this information just like the clearinghouse would. Furthermore, they would have to share this information upon request of the clearinghouse. For example, the clearinghouse would want to know what project a slice was bound to, and that may not be clear unless that becomes part of the slice credential.

Resource Discovery

The clearinghouse will provide experimenters with mechanisms to discover components as a clearinghouse for all the resources available in the federation, and this is actually from where the name "clearinghouse" is derived. One goal here is to provide a mechanism for slice owners to determine whether an aggregate has signed the aggregate provider agreement, but this service is also congruent with future goals of providing optional portal tools on the clearinghouse for the full experiment lifecycle management. By implementing this as a trusted directory service, both the goal of verifying an aggregate is "GENI-approved" and helping slice owners easily find aggregates can be met with one service.

This list maintained in the component registry will not provide real-time availability of resources. The experimenter, perhaps with help from clearinghouse portal tools, will have to go directly to the aggregate to reserve resources for specific time-periods. While the clearinghouse does not and cannot act as a scheduler for the aggregates, it would be beneficial to keep this information as accurate as possible. Aggregate operators are encouraged to inform the clearinghouse of planned or unplanned long term outages. Also, as part of the aggregate provider agreement they agree to inform the clearinghouse when resources are permanently retired so that they can keep the registry clean. Of course, all of this means that the resource discovery service is best effort, and operational problems with specific components should still be directed to the appropriate aggregate operator.

It should be noted that the primary purpose of discovering which aggregates are GENI endorsed, i.e. signed the aggregate provider agreement, could be achieved without a resource discovery process and complete component registry. For example, ABAC could be used where the clearinghouse asserts that aggregates are "official", and they could then use this attribute to prove that they are registered aggregates to the slice owners. These solutions are not mutually exclusive either.

Federation Resource Allocation Policy Verification

Resource allocation policies may come from the GENI Oversight Group through NSF or through special agreements with other identity portals, such as, FIRE. The first kind of policy should be either listed in this document's policy section or referenced in this document as an external policy. Currently, there are no such policies, but an example policy might be something like, "students are only allowed to have 10 hosts per slice that they create". The second type of policy would be in agreements that should be publicly available on the clearinghouse web site. Examples would be a limit on slice size for FIRE users or a limit on bandwidth usage by GENI users for an international link with FIRE. Potentially, any aggregate authority could negotiate some agreement like that on resource usage by GENI slices, which could be verified at the clearinghouse.

Because individual aggregates are autonomous and free to allocate resources to whomever they please, **this is policy verification and not enforcement**. The service provided by the clearinghouse is to give information to any aggregate as to whether or not a resource request for a

slice would violate such federation policies. This is necessarily a best effort service because the clearinghouse will rely on aggregates to inform it **after the fact** of resources allocated for slices endorsed by the clearinghouse. Aggregate authorities have agreed to provide this information as part of the Aggregate Provider Agreement.

Some aggregates, such as the GENI Racks, will only accept resource requests through the clearinghouse. They will then implicitly receive only compliant requests. Other aggregates will accept requests directly from the experimenters. An interface to the clearinghouse will be provided to them to check policy compliance of a request in real-time should they choose to use it. **A separate interface will be provided to aggregates to inform the clearinghouse of allocation requests granted, ideally, the same non-blocking interface that they would use to send such information back to the relevant slice authority.**

It seems to be agreed that if it all possible, resource allocation policies should be verified at the aggregates or slice authorities instead of the clearinghouse. For example, a policy about how many resources a particular class of slice or experimenter could reserve is within the issuing slice authority's capabilities of checking. So such policies could be pushed out to trusted SAs. A policy such as GENI slices in total can only use at most X% of a given aggregate, such as a FIRE link, is something that aggregate can check. The only policies that cannot be checked are of the form that require looking at the resources from multiple slices spanning SAs regarding constraints about component usage spanning multiple aggregates. An example would be "the combined usage of GENI low priority slices cannot use more than 50% of critical resources (e.g., GENI racks and network backbone links). That policy would require an entity with a view broader than one aggregate manager or slice authority. If we do not think there are use cases for any such policy, then we should not add in this complication of running a global slice tracker at the clearinghouse which could be costly as well as introduce inefficiencies such as reporting back duplicate information to SAs and the clearinghouse.

Future Services

This clearinghouse policy is a living document. As new services and responsibilities are added to the role of GENI Clearinghouse, this document must be updated. There are several services that have been discussed, but not deemed critical to implement any time soon. These include experiment sunseting and archiving, experiment template creation, and several deployment tools to make the creation of new experiments simpler. If the clearinghouse is ever expanded into a more general portal with these services, descriptions of the services and quality of service guarantees will need to be added here. Furthermore, privacy policies will need to account for any new types of data collected.

5. Policies

In this section we describe the policies that guide the operations of the clearinghouse. The service level promises are not in this section, but are instead discussed in section 4 along with the descriptions of each service.

Governance

The GENI Clearinghouse receives its direction from the GENI Oversight Group (GOG), which is to be established in the federation charter. Until the GOG is established, the GPO fulfills the role. The Clearinghouse Operator manages the Clearinghouse Operations Team to fulfill its mission as handed down from the oversight group and described in this document.

The clearinghouse does not have direct authority over any other party. Instead, agreements are established with the community it serves, and if agreements are violated, it may stop providing services to or endorsement of those parties. For example, the Aggregate Provider Agreement sets a standard of service that aggregates will provide to the GENI community. If they cannot maintain the security and integrity of their services, then they could be delisted in the clearinghouse with attributes revoked. Similarly, an experimenter could use a slice maliciously and violate the AUP. In that case their GENI identity credential, if generated by the clearinghouse, could be revoked. If another identity portal issued the credential, they would need to revoke the credential, at least the GENI credentials/attributes. They could still hand out credentials to that user for their own test bed, for example. Again, this would only be enforceable through agreements: the identity portal agreement with the clearinghouse in this case.

Responsibilities

The clearinghouse's responsibilities to the community (e.g., the services it will provide and the way it protects personal information) are described in this document. The responsibilities of the other actors (e.g. aggregate authorities, identity providers and experimenters) towards the community are to be spelled out in agreements they sign with the clearinghouse.

The parties that ultimately bear responsibility for the behavior of an experiment are the experimenter and project lead, as spelled-out in the AUP, project leader agreement, and Legal, Law Enforcement and Regulatory Plan. The project leader is expected to delegate slice creation capabilities to trusted individuals with due care, and the project leader is expected to be aware of the different experiments and experimenters associated with their project. The experimenter who runs the actual experiment within a slice is most directly responsible for the behavior of a slice, particularly in regards to careless, disruptive or illegal activities of an experiment. However, it may not always be possible to determine more than the project leader and slice owner. Individual aggregates are not in the position to take responsibility for experiments as they are not given the information to be aware of exactly what experimenters are doing with their resources. All that an aggregate operator can do is shut down slivers if informed by another, such as a law enforcement agency, that a slice is misbehaving. Through all of this, the GENI LLR Representative has the responsibility to route requests and put the different parties in contact to resolve problems but again is not responsible for the behaviors of the experiments.

Conflict Resolution Process

The clearinghouse could take actions against slices, experiments, project leaders and aggregates based upon violations of agreements or under the order of a court in rare circumstances. The clearinghouse may:

- Delist an aggregate's resources from the component registry or revoke endorsements given to the aggregate;
- No longer endorse an identity portal for authentication and/or credential creation and revoke attributes given to it;
- Revoke or deregister a slice (unless it has delegated this to Slice Authorities);
- No longer endorse a slice authority for credential creation and revoke any attributes given to it;
- Revoke any project credentials/attributes given; and
- Revoke a GENI identity credential for an experimenter or project lead if the clearinghouse was the identity portal.

These are the only tools available to the clearinghouse for enforcement of agreements. Directions to take such actions could come from the GENI Oversight Group, a law enforcement agent with proper authority and documentation, or the Clearinghouse Operator if they determine an agreement has been violated. However, there is a process that is followed to try and resolve conflicts before any such actions are taken, and there are mechanisms of appeal for any decision. The process will follow these steps for any violation or complaint of a violation.

1. A complaint is made with the clearinghouse by a GENI actor or an LLR (Legal, Law Enforcement & Regulatory) agent.
2. The clearinghouse operator reviews the complaint and tries to gather information regarding the validity of the complaint. She may consult with a lawyer in the case of an LLR request, with the assistance of the GENI LLR Representative.
3. The clearinghouse operator informs the accused actor of the complaint and let's them respond. Unless there is some legal reason that they cannot inform the accused or must act more quickly than the accused can respond, they will wait for a response.
4. The clearinghouse operator, perhaps with guidance from the GENI Oversight Group, will make a decision. If the complaint came with a directive to take action from the GENI Oversight Group directly, steps 2 and 3 may be skipped.
5. The response is disseminated to all parties involved and carried out. This whole process will be as open and transparent as legally possible in all situations.

Those who are accused of breaking an agreement and have had credentials or services revoked can always make an appeal to the GENI Oversight Group who will have the final say on any decisions regarding the above actions that could be taken by the clearinghouse. The following steps are taken in the case of an appeal.

1. The GENI Oversight Group receives an appeal.
2. The oversight group informs the clearinghouse. They may or may not request a stay on an action taken while the appeal is being reviewed.
3. The oversight group gathers as much information as possible from all relevant parties and makes a decision.
4. The decision is communicated to the party making the appeal and the clearinghouse operator, who will follow their decision.
5. If the appeal is not resolved in favor of the accused, they are given instructions on what they must do to resolve the problem and reverse the action. Except for serious legal issues, it is unlikely that anyone would be permanently removed from the federation. However, to rejoin they would need to address the issues that were considered breaches of their agreements.

Privacy Policy

The clearinghouse respects the privacy and rights of its users and recognizes the responsibility and trust put in it by the community. Therefore, every effort is made to protect that privacy.

The clearinghouse collects information at registration for attribution and generates logs of all transaction (e.g., registering slices, creating credentials, generating attributes, etc) performed while providing its services. These logs will be stored for at least 90 days. Clearinghouse operations uses this information only to provide for the security and operational stability of GENI and to determine the parties responsible for the actions of a given slice. Identifying information is never shared to those not providing GENI operational services, unless legally required, and never for anything beyond providing secure and highly available services. If identifying information is ever shared in such cases, effort is made to inform the identified party of exactly what was shared and why.

The clearinghouse follows the Legal, Law Enforcement and Regulatory (LLR) Plan, and may receive requests from an LLR agent either directly or referred from the GENI LLR Representative. **If the clearinghouse is asked who the owner of a slice is, it will first offer to point the requestor to the email alias created for each slice when it is first registered.** If the clearinghouse does not have full contact information on the user, it may redirect the request to the appropriate identity portal who will follow their institutional policies on releasing such information. If ordered by a court or recommended by legal council for the institution operating the clearinghouse, they will reveal full contact info to the LLR agent making the request. However, they will also inform the user that they have done so unless legally prohibited from doing so.

The clearinghouse may collect certain attributes for verification of resource allocation policies. Attributes regarding role (e.g., project leader, slice owner, or student), institution type (e.g., EDU, corporate, or government lab), and common name may be bound with credentials and passed on to other GENI entities. Attributes with contact information may be used to contact a person in the event of a problem, or to route requests to appropriate parties as described in the Legal, Law Enforcement and Regulatory Plan. Other attributes, if collected, will not be passed on or released by the clearinghouse and may only be used for verification of global resource allocation policies.

Finally, the clearinghouse operations team will take due diligence and follow industry best practices to secure the registries and logs against attackers. They will follow hardening guidelines if developed by the GENI Computer Security and Incident Response Team (GENI-CSIRT). Furthermore, if these databases ever do become compromised and there is reason to believe identifying information is exposed, the affected users will be promptly notified.

Identity Providers

GENI Identity Portals must use an approved Identity Provider or become one themselves. Identity providers are approved by the GOG. Currently, InCommon is the only approved identity provider.

Updating this Policy

Any changes to this policy, once it is no longer a draft, will have to go through the following process for acceptance.

1. Recommended changes must be disseminated to all GENI stakeholders who might enter into agreement with the clearinghouse. This can be done at a GEC or through email.
2. There will be an open comment period of at least 6 weeks.
3. Recommendations may be incorporated into a new recommended version which will be disseminated to all.
4. The GENI Governance Group will either approve or disapprove. If they disapprove, their issues must be addressed and we start back at step 1.

Aggregate Provided Data

Because some aggregates will not require resource requests to come through the clearinghouse, the clearinghouse will not see all resource allocations to slices. Without knowing what resources are given to a slice, it would have no way to verify **all** potential federation level resource allocation policies are actually being followed. Therefore, aggregates are required per the Aggregate Provider Agreement to provide the clearinghouse with information regarding requests they have granted for GENI slices, i.e. those registered and signed by the clearinghouse. This would be the same information that they provide back to the slice authorities asynchronously.

In addition to resources allocated, aggregates should be providing the clearinghouse with updates on resources that malfunction, go offline or are retired (the latter required per the Aggregate Provider Agreement). While in theory the clearinghouse could regularly ping components, that is costly to do frequently for a large set of components. Therefore, it is more efficient to operate under the assumption that resources are operating normally, unless notified by an aggregate operator.

Lastly, it is requested that aggregate operators provide the GMOC a list of all publicly facing IPs potentially used by its slivers. By having a list of public IPs that are associated with GENI experiments, the LLR representative can respond to requests more efficiently and promptly. However, this is not required in the Aggregate Provider Agreement because it may not always be technically possible.

Information regarding the status aggregates (e.g., retired, online, offline, etc) are public and may be integrated into the directory of aggregates/components that are endorsed by the clearinghouse. Information regarding resources allocated to specific slices is not shared by the clearinghouse but only used internally to verify policy.

If there are no use cases for policies that could only be verified at the clearinghouse, then the requirement to send duplicate information back to the clearinghouse should be removed. In all cases envisioned to date, it seems that slice authorities or aggregate managers could enforce policy instead.

Certificate Authority Policy

Since the clearinghouse is issuing credentials, signing others credentials and acting as a trusted root or bridge between entities, it is very much acting like a CA (certificate authority). It is not unique in this manner as identity portals and slice authorities also issue credentials or sign assertions, but it is unique in the sense that it is a trust anchor for the whole federation.

For the moment, there are few enough organizations issuing credentials that trust can be established more ad hoc. However, GENI could expand to the point where credential issuing entities do not really know each other any more. At that point, it would be prudent to develop a formal certificate authority policy to guide how the clearinghouse will vet users and protect cryptographic materials, which should then be adopted by all actors issuing similar credentials in the federation. If such a policy is developed, it will be referenced in this section, but remain separate from this clearinghouse policy document.

Glossary

- **Aggregate:** is a system containing a collection of resources (i.e. components) under common administration running an aggregate manager service (defined in the GENI Software Framework Architecture).
- **Aggregate Authority (AA):** is responsible for the management of the aggregate, but can delegate selected functions to other actors. The aggregate authority is the only one who can enter into agreements for the aggregate.
- **Aggregate Administrator:** is one who has been delegated the responsibility, by the aggregate authority, to set local resource allocation policy for an aggregate and its components.
- **Aggregate Operator:** is appointed by the Aggregate Authority to operate the Aggregate Manager and any components of the aggregate. This may be the AA itself, or someone from another organization operating on its behalf.
- **Component:** encapsulates a collection of resources, including physical resources (e.g., CPU, memory, disk, bandwidth) logical resources (e.g., file descriptors, port numbers), and synthetic resources (e.g., packet forwarding fast paths).
- **Component Registry:** holds or points to a record for each affiliated substrate component or aggregate. Each record includes: the responsible organization (i.e., aggregate authority); associated principals (e.g., operators) and their individual permissions; the interface(s) to query for available resources (e.g., on the aggregate manager); other contact information; and (optionally) policy to be applied to use of this component or aggregate.
- **Clearinghouse:** is both an entity and a system consisting of software, operations, and policy to enable authoritative resource allocation in a GENI federation.
- **Clearinghouse Operations:** is the operations team responsible for the GENI clearinghouse. This could be a role of the GENI meta-operations group. The **Clearinghouse Operator**, is the one managing this team.
- **Experimenter:** is a user with credentials recognized by a slice authority (possibly the clearinghouse itself) to act upon a slice.

- **GENI-CSIRT:** Computer Security and Incident Response Team for GENI composed of people from several major stakeholder institutions and guided under the authority of the GENI Oversight Group.
- **GENI Project:** is a grouping of experimenters and slices working on a common effort. It may have multiple slices concurrently and over time.
- **GENI Oversight Group:** is the group responsible for ensuring that meta-operations and the clearinghouse operations groups fulfill their responsibilities. It is also the governance body for the GENI federation, responsible for guiding project direction and resolving disputes between other actors.
- **Identity Portal:** is a trusted (i.e., one that has signed an agreement with the clearinghouse to collect and verify attributes, use approved identity providers, present users with the AUP, and log credential creation) system that issues GENI credentials for principals.
- **Identity Portal Authority:** is one who can form agreements with other GENI actors on behalf of the identity portal.
- **Identity Portal Operator:** is one who has been delegated the responsibility for maintaining the operational readiness of that identity portal.
- **Identity Provider:** is a service providing authentication of potential GENI actors. User registration, vetting, enrollment, and attribute collection will often be exported to an identity provider, such as InCommon, rather than requiring attribution at the identity portal who's main job is minting GENI credentials for those who accept the presented GENI AUP.
- **Meta-operations:** is the operational group responsible for cross-aggregate issues & experimenter support.
- **Project Leader:** is the actor who is ultimately responsible for the behavior of a GENI project.
- **Principle Registry:** holds or points to a record for each GENI-associated experimenter, project leader, operator, etc. Each principal record includes: a global name, contact information, authentication key (or a pointer to it in another trusted registry), roles, and status (active, suspended, etc.). Depending upon the agreements with an identity portal, the registry may be split across the identity portal and the clearinghouse.
- **Slice Authority:** is a system that issues credentials for slices. There are minimal requirements, (such as supporting revocation), needed of slice authorities, but slices are not trusted by GENI until the clearinghouse registers the slice and signs it. However, agreements with slice authorities could give them extra authority to act on the clearinghouse's behalf and "register" slices through an asynchronous ABAC, (or similar), mechanism.
- **Slice Registry:** holds or points to a record for each slice, equivalent to a "bank account" for that slice in that it records transactions and authorized accesses. Each slice record includes: the responsible organization (e.g., the slice creator) and its permissions; the associated GENI project; associated principals (e.g., experimenters) and their individual permissions; and the slice status (active, suspended, etc.).